RECEIVED
CENTRAL FAX CENTER
OCT 0 5 2006

KILPATRICK
STOCKTON LLP
Attorneys at Law

Suite 900 607 14th St., NW
Washington DC 20005-2018
t 202 508 5800 f 202 508 5858
www.KilpatrickStockton.com

direct dial 202 508 5883
direct fax 202 585 0041
MDimino@KilpatrickStockton.com

October 5, 2006

FAX

RECIPIENT/ PHONE NO.	3 FAX NO.	COMPANY/ CITY, STATE, COUNTRY
Scott L. Jarrett - TC 3600 GROUP ART UNIT 3623 571 272 7033	571 272 7033 571 2738300	USPTO

COMMENTS RE SAIC0039 – SERIAL NO. 09/805,279

Examiner Jarrett,

Thanks for agreeing to meet with us this afternoon regarding U.S. Patent Application No. 09/805,279. We hope to come to a common understanding of the Shrader reference and its applicability to the claims.

I've included a brief version of our analysis of Shrader as applied to Claims 29 and 33 of the application.

Tom Corrado and I look forward to meeting with you today at 2:00 p.m.

Very truly yours,
Mike Dimino
(202)714-5007; 44,657

Michael J. Dimino FROM	4 PAGES (WITH COVER)
1615 REFERENCE NO	36609/204105 CLIENT/MATTER NO.

PLEASE CALL 202 508 5816 IF YOU HAVE DIFFICULTY WITH THIS TRANSMISSION.

TO BE COMPLETED BY KS OPERATIONS CENTER

TRANSMISSION RECEIPT DATE/TIME: _____

COMPLETED BY: _____ **JOB CODE** _____

PAGE 1/4 * RCVD AT 10/5/2006 11:31:46 AM [Eastern Daylight Time] * SVR:USPTO-EFXRF-2/9 * DNIS:2738300 * CSID:2025085858 * DURATION (mm-ss):01-34

Claim 29, 33 as being anticipated by Shrader

A method for verifying a cast ballot B_{cast} stored in a server, the method comprising:

Shrader does not disclose a method for **verifying** a cast ballot in a server. "Verification," as an activity in the application, is initiated by a user after obtaining a confirmation token from a system of the invention:

> *[0004] ... "verifiability" (everyone should be able to verify their own ballot ...*
>
> *[0060] Descriptors 71 and 73 illustrate what is known as individual verifiability[1] ...*
>
> *[0019] ... the terms "individual", "user", "client", and "voter" are used interchangeably, and refer to a **person** ...*

Shrader discloses verification by a combination of a "tabulator" and a "mediator," two servers in a Shrader system. *See e.g.*, Schrader [0063].

Most of the portions of the Shrader cited in the 07/11/06 OA (Abstract; [0050]-[0053]; [0060]-[0062]; Figures 4-8) do not mention verification even in the above inapplicable manner.

forming a digital signature of B_{cast} using a private key of the server $DS(B_{cast}, s)$;

Shrader does not disclose a server signing a cast ballot B_{cast}. In the application, B_{cast} represents the actual votes.

> *[0052] ... The cast ballot Bcast 51 is structured in a way that it is easy to read the response values and determine which issues or offices were being voted on, **and what the selections were.***

In Shrader, the tabulator signs the **empty ballot** as part of validation.

---

[1] "Individual" verifiability is what is claimed in Claims 29 and 33. The other sort of verifiability is "universal" and does not require a confirmation token.

[0062] ... Voting entity casts its votes 66 and encrypts the votes and the encrypted electronic ballot

This clearly shows that the votes and the ballot are two separate things. Later Shrader uses the private key of the tabulator to encrypt the **empty ballot**, not the votes:

[0063] ... The voting tabulator signs, encrypts and sends the encrypted ballot to the voting mediator in a message that is encrypted with the voting mediator's public key and signed with the voting tabulator's private key.

The 07/11/2006 OA also cites Figures 7-8 element 72 as applicable. Those drawings provide no applicable disclosure.

That Shrader's **ballot** does not contain votes (as the present application's Bcast does) is even more apparent a few sentences later when Shrader **teaches away** from the next limitation.

associating B_{cast} and $DS(B_{cast}, s)$ with a vote serial number (VSN);

Shrader does not disclose associating B_{cast} and $DS(B_{cast}, s)$ with a vote serial number (VSN). In fact, Shrader **teaches away** from this approach:

[0063] ... The verification message does not contain the actual votes from the ballot, since the voting must be anonymous.

forming a confirmation token, comprising DB(Bcast, s) and VSN;

The 07/11/2006 OA cites [0061]-[0063] and Figures 7-8 as disclosing this limitation. As noted above, in [0063] Shrader teaches away from relating the cast ballot (actual votes) with an identifier like a Vote Serial Number.

making the confirmation token available to a user; receiving a confirmation token made available to a user;

The 07/11/2006 OA asserts that Shrader's disclosure of a verification message between two servers (the tabulator and the mediator) in [0063] constitutes making the confirmation token available to a user. In addition to the fact that Shrader does not form a confirmation token as that term is defined in the Claims, it has been shown that a server is not a "user"

> *[0019] ... the terms "individual", "user", "client", and "voter" are used interchangeably, and refer to a person ...*

The confirmation token that Shrader doesn't disclose isn't made available to a user; so it's difficult to see how the nonexistent unavailable token can then be received by the server. Each of these steps is required by the claims.

extracting $VSN_{received\ token}$ and $DS_{received\ token}(B_{cast}, s)$ from the received token;

With no token having been created containing elements that Shrader teaches away from combining, and with the non-created token not having been available to a user who didn't return it, it's not possible for a Vote Serial Number and Cast Ballot (signed with the private key of the server) to be extracted from such a token.